AMENDMENTS TO THE SPECIFICATION

Amend the paragraph beginning on page 10, line 4, as follows:

Through the cooperating the modules described above, the wireless security component 202 is able to efficiently manage threats posed by unauthorized wireless network devices in a passive manner. FIGURE 5 is a flow diagram illustrating an exemplary routine 500 for passively monitoring for wireless device threats on the network. Beginning a block 502, the wireless security component 202, begins to passively monitor for new wireless device activity. For purposes of the present discussion, passively monitoring for wireless device activity means that the wireless security component 202 examines network traffic, or frames, as they are transmitted by the various devices on the computer network 200 in their normal course of operation. This passive monitoring is in contrast to actively, and indiscriminately, causing network devices to transmit information, and then examining the resultant traffic for any wireless devices. By passively monitoring for network traffic from unknown wireless devices, the overall system performance of the computer network 200 is not adversely ~~impacting~~ impacted.

Amend the paragraph beginning on page 10, line 25, as follows:

At block 506, the responses from the wireless device are received. At block 508, information contained in the responses is collected and analyzed, from which a device profile that attempts to uniquely ~~identifies~~ identify the unknown wireless device is generated. While the illustrative routine 500 shows that only one query is sent, this is for illustration purposes, and should not be construed as limiting upon the present invention. The queries are designed to elicit responses from the unknown wireless device which can be used to uniquely identify the unknown wireless device based on identifying characteristics in the response. Thus, according to one embodiment, multiple queries are sent to the wireless device in order to determine the unique device profile. Further, based on the response from a first query, a second query is determined and sent. For example, based on a response to a request for the operating system, a specific

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

request known to be supported by the reported operating system may follow. This process of determining a unique device profile is referred to as probing the device.

Amend the paragraph beginning on page 11, line 6, as follows:

While probing an unknown wireless device cannot strictly be viewed as an entirely passive process, it should be understood that, in contrast to indiscriminately requesting device information from the entire network, and filtering information from the resulting responses, probing is specific to, and directed at, a particular wireless device, and efficiently queries the device to determine the unique device profile. Thus, very little actual network traffic is generated by a probe, [[an]] and the actual impact on the computer network is negligible.

Amend the paragraph beginning on page 12, line 3, as follows:

At block 516, a system journal is updated with the threat level for the unknown wireless device. Optionally, at block 518, a threat management routine is initiated to handle the threat established for the unknown wireless device. For example, while the above-mentioned threat management routine may execute at given intervals, if a given threat threshold is established for the unknown wireless device, the routine 500 may cause [[that]] the above-mentioned threat management routine to execute immediately. An exemplary threat management routine is described below in regard to FIGURE 6. Additionally, or alternatively, (not shown) a warning message may be sent to the system administrator via the administrator console 406, advising the system administrator of the detected threat. Thereafter, the routine 500 terminates.

Amend the paragraph beginning on page 13, line 1, as follows:

FIGURE 7 is a flow diagram illustrating an exemplary sub-routine 700 for processing [[an]] a threat posed by a wireless device, suitable for use by the management routine 600 of FIGURE 6. Beginning at block 702, information regarding actions to be taken when wireless devices pose a particular threshold is retrieved. As previously indicated, these thresholds may be based on a variety of criteria and recommend numerous actions to be taken. For example, when an unauthorized/unknown wireless computing device comes within range of an authorized wireless access point, the computing device will identify itself to the wireless access point. This

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682 8100

may merit a minimal, or low, threat level and no action is required. However, if that same unknown wireless computing device attempts thereafter to access files within the network, the threat level may then be raised to a very high level, and exceeding a predetermined threshold, appropriate blocking actions may be taken. In this fashion, the present invention may be thought of as a just-in-time security system. Alternatively, if a printer is connected to the network over a wireless connection, a minimal threat level is established and no action is required. As yet a further alternative, if a new wireless access point is detected, this may merit an immediate high threat level due to the enhanced security risks posed from other unknown wireless devices, and, exceeding a predetermined threshold, a high priority warning message is sent to the system administrator to take appropriate action.

Amend the paragraph beginning on page 14, line 8, as follows:

Alternatively, if the device is not to be de-authorized, at decision block 714, a determination is made as to whether there should be an additional probe may be made on the device. This additional probe may be made to further determine the ~~identify~~ identity of the device, or specific details that may be subsequently used in evaluating the threat level posed. If no additional probe is required, at block 706, the system journal is updated, and the routine 700 terminates. However, if an additional probe would be appropriate, at block 716, the wireless device is again probed for its unique characteristics, which are recorded with its device profile in the device profile database. Thereafter, at block 706, the system journal is updated, and the routine 700 terminates.

Amend the paragraph beginning on page 18, line 17, as follows:

In addition to allowing, or disallowing, network traffic to flow to the wired network zone 110, the bridge/probe module 404 analyzes the network traffic ~~travelling~~ traveling between the wireless and wired network zones, summarizes the analysis, and forwards it to the administrator module 406 for system administrator purposes. Types of information collected from wireless devices and wireless access points include gateway and DHCP server location, hardware manufacturer, and the like.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100